AMENDMENTS TO THE CLAIMS

1. *(Currently Amended)* Method for secure wireless transmission of information from a ~~sender~~digital pen to a ~~receiver~~ receiving device, comprising:

obtaining, in the digital pen, a message ~~and a receiver identity in a sending device~~ in the form of a plurality of absolute positions recorded from an absolute position coding pattern on a substrate;

obtaining, in the digital pen, at least one absolute position recorded from an absolute position coding pattern on a secure note;

sending said at least one absolute position recorded from the secure note to a database device, in which said at least one absolute position is associated with an address of the receiving device;

receiving, in the digital pen, said address and an encryption key of said receiving device, from the database device;

encrypting the message to be transmitted using said encryption key received from the database device;

obtaining a transmission channel from the ~~sending device~~ digital pen to ~~a~~ the receiving device;

~~obtaining a receiving address from a secure note, in which a pattern is connected to a receiving device;~~

transmitting the encrypted ~~information~~ message to the receiving device;

decrypting the information in the receiving device;

presenting the message to ~~the~~ a receiver; and

optionally acknowledging the receipt of the message to the ~~sender~~ digital pen.

2.-4. *(Canceled)*

5. *(Currently Amended)* Method as claimed in ~~claim 2~~1claim 1, further comprising ~~the step~~:

encrypting the message in the ~~sending device~~ digital pen by a symmetric key and decrypting the message ~~by~~ in the receiving device by the same key.

6. *(Currently Amended)* Method as claimed in claim 5, wherein the symmetric key has been agreed upon in advance and is stored in the ~~sending device~~ digital pen and the receiving device.

7. *(Currently Amended)* Method as claimed in claim 5, further comprising ~~the steps~~:

adding the symmetric key to the message after encryption with the symmetric key,

encrypting at least the symmetric key by a public key of an asymmetric key having a private key and a public key and belonging to the ~~receiver~~ receiving device,

decrypting the symmetric key by the private key of the ~~receiver in the~~ receiving device; and

using the symmetric key for decrypting the message.

8. *(Currently Amended)* Method as claimed in claim 7, further comprising ~~the steps~~:

encrypting the already encrypted symmetric key in the ~~sending device~~ digital pen by a private key of an asymmetric key having a private key and a public key and belonging to the ~~sender~~ digital pen~~,~~;

obtaining, in the receiving device, the ~~sender~~ digital pen public key from one of the digital pen and ~~by the receiving device, such as from the sending device or~~ a separate server; and

decrypting the symmetric key by the public key of the ~~sender~~ digital pen in the receiving device and by the private key of the ~~receiver~~ receiving device.

9. *(Currently Amended)* Method as claimed in ~~claim 1~~claim 27, further comprising ~~the step~~:

identification of a user of the ~~sender~~ digital pen to the ~~sending device~~ digital pen, and/or identification of the receiver to the receiving device by a verification means, ~~such as~~ wherein the verification means is at least one of PIN-code, optical, sound, vibration, heat, speed, angle, time, pressure, acceleration,

absolute coordinate, handwritten signature, voice recognition, fingerprint sensor, ~~or~~ and other biometric means.

10. *(Currently Amended)* Method as claimed in ~~claim 1~~claim 9, further comprising ~~the step~~:

obtaining a random seed for generating encryption key by means of the verification means during the identification step.

11. *(Currently Amended)* Method as claimed in ~~claim 1~~claim 27, further comprising ~~the step~~:

obtaining a random seed for generating an encryption key during the step of obtaining the message.

12. *(Currently Amended)* Method as claimed in ~~claim 1~~claim 27, further comprising ~~the step~~:

generating, in the ~~sending device~~ digital pen, a digital pen ~~sender~~ private key and ~~sender~~ digital pen public key pair using a random seed obtained using a physical parameter relating to the user of the ~~sender~~ digital pen, ~~such as~~ wherein the physical parameter is at least one of handwritten signature recognition, fingerprint information ~~or~~ and movement of the ~~sending device~~ digital pen ~~or of the sending device, such as~~ wherein movement of the digital pen is at least one of acceleration, speed, time, and vibration ~~etc~~.

13. *(Currently Amended)* Method as claimed in claim 12, wherein the ~~sender~~ digital pen ~~public~~ private key is added to the message unencrypted, as ~~sender~~digital pen identification.

14. *(Currently Amended)* Device for secure wireless transmission of information from a ~~sender~~ digital pen to a ~~receiver~~receiving device, comprising:

~~a sending device arranged for obtaining a message and a receiver identity;~~

a substrate provided with an absolute position coding pattern coding absolute positions,

a secure note provided with an absolute position coding pattern coding at least one absolute position,

a database device, in which said at least one absolute position is associated with an address of the receiving device,

a digital pen configured for obtaining a message from the absolute position coding pattern of said substrate and for receiving said address of the receiving device from the database device,

encryption means, in the digital pen, for encrypting the message to be transmitted by an encryption key received from the database device;

a transmission channel from the ~~sending device~~ digital pen to the ~~a~~ receiving device for transmitting the encrypted ~~information~~ message to the receiving device;

decryption means for decrypting the information in the receiving device; and

display means for presenting the message to ~~the~~ a receiver~~,~~ ~~and~~

~~a secure note, in which a pattern is connected to a receiving device~~.

15. *(Canceled)*.

16. *(Currently Amended)* Device as claimed in ~~claim 15~~claim 14, wherein the receiving address is obtained by transmitting said at least one absolute position coded on the secure note to the ~~a~~ database device, ~~in which the absolute position code is associated with said one receiving address,~~ and using said receiving address for the transmission.

17. *(Canceled)*.

18. *(Currently Amended)* Device as claimed in claim 14, wherein the encryption means is arranged to encrypt the message in the ~~sending device~~ digital pen by a symmetric key and that the

decryption means is arranged to decrypt the message in the receiving device by the same key.

19. *(Currently Amended)* Device as claimed in claim 18, wherein the symmetric key has been agreed upon in advance and is stored in the ~~sending device~~ digital pen and the receiving device.

20. *(Currently Amended)* Device as claimed in claim 18, wherein

the symmetric key is added to the message after encryption with the symmetric key;

the encryption means is arranged to encrypt at least the symmetric key by a public key of an asymmetric key having a private key and a public key and belonging to the ~~receiver~~ receiving device;

the decryption means is arranged to decrypt the symmetric key by the private key of the receiver in the receiving device; and

the decryption means is arranged to use the symmetric key for decrypting the message.

21. *(Currently Amended)* Device as claimed in claim 20, wherein

the encryption means is arranged to encrypt the already encrypted symmetric key in the ~~sending device~~ digital pen by a private key of an asymmetric key having a private key and a public key and belonging to the ~~sender~~ digital pen,

the receiving device is arranged to obtain the ~~sender~~ digital pen public key, such as from the ~~sender~~ digital pen or a separate server; and

the decryption means is arranged to decrypt the symmetric key by the public key of the ~~sender~~ digital pen in the receiving device and by the private key of the ~~receiver~~ receiving device.

22. *(Currently Amended)* Device as claimed in claim 14, further comprising:

a verification means for identification of a user ~~the sender~~ to the ~~sending device,~~ digital pen and/or identification of ~~the~~ a receiver to the receiving device, said verification means being arranged to use identification measures~~, such as~~ wherein the identification measures are at least one of a PIN-code, optical, sound, vibration, heat, speed, angle, time, pressure, acceleration, absolute coordinate, handwritten signature, voice recognition, fingerprint sensor, ~~or~~ and other biometric means.

23. *(Currently Amended)* Device as claimed in ~~claim 14~~claim 22, further comprising:

encryption key generation means for obtaining a random seed for generating encryption key by means of the verification means during the identification step.

24. *(Original)* Device as claimed in claim 14, further comprising:

encryption key generation means for obtaining a random seed for generating an encryption key during the step of obtaining the message.

25. *(Currently Amended)* Device as claimed in claim 14, wherein the ~~sending device~~ digital pen is arranged to generate a ~~sender~~ digital pen private key and ~~sender~~ digital pen public key pair~~, and is arranged to use~~ using a random seed obtained using a physical parameter relating to a user of the ~~sender~~digital pen, ~~such as~~ wherein the physical parameter is at least one of handwritten signature recognition, fingerprint information~~, or~~ and movement of the digital pen~~sending device or of the sending device, such as~~ wherein movement of the digital pen is at least one of acceleration, speed, time, and vibration~~etc~~.

26. *(Currently Amended)* Device as claimed in ~~claim 26~~claim 25, wherein the ~~sender~~ digital pen ~~public~~ private key is added to the message unencrypted, as ~~sender~~ digital pen identification.

27. *(New)* A method for secure transmission of information from a digital pen to a receiving device, comprising:

obtaining, in the digital pen, a message in the form of a plurality of position indications recorded from a position code on a substrate;

sending at least one of said position indications to a database device;

receiving from the database device an address of a receiving device which is associated with the at least one position indication and an encryption key relating to said receiving device;

encrypting said message using the encryption key received from the database device; and

transmitting the encrypted message to the address of the receiving device.

28. *(New)* A method as claimed in claim 27, wherein the encryption key is a public key of an asymmetric key pair belonging to the receiving device.

29. *(New)* A method as claimed in claim 27, wherein the step of sending further comprises sending an identity of the pen to the database device.

30. *(New)* A method as claimed in claim 27, wherein the step of encrypting further comprises encrypting the message in the digital

pen by a symmetric key before encrypting the message with the encryption key received from the database device.

31. *(New)* A method as claimed in claim 30, wherein the symmetric key is added to the encrypted message before encrypting it with the encryption key received from the database device.

32. *(New)* A method as claimed in claim 27, wherein the step of transmitting comprises transmitting an identity of the pen to the address of the receiving device.

33. *(New)* A method as claimed in claim 27, further comprising displaying the address of the receiving device to a user of the digital pen and obtaining one of a confirmation and a rejection of the address from the user.

34. (*New*) A method as claimed in claim 27, wherein at least one of the sending step, the receiving step and the transmitting step is carried out over a network.

35. (*New*) A system for secure transmission of information from a digital pen to a receiving device, comprising:

a digital pen, which is configured to obtain a message in the form of a plurality of position indications recorded from a

position code on a substrate and to send at least one of the position indications to a database device; and

a database device, which stores an address of the receiving device associated with said at least one of the position indications, and which is configured to send an encryption key relating to the receiving device and the address of the receiving device to the digital pen in response to the receipt of said at least one of the position indications,

said digital pen being further configured to encrypt the message using the encryption key received from the database device and transmit the encrypted message to the address of the receiving device.

36. (*New*) A system as claimed in claim 35, wherein the digital pen has a pen identity, which is sent to the database device together with said at least one of the position indications.

37. (*New*) A system as claimed in claim 35, wherein the database device is configured to send an encryption key belonging to the digital pen to the receiving device.

38. (*New*) A system as claimed in claim 35, wherein the digital pen stores a public key of an symmetric key pair belonging to the database device.

39. (*New*) A method as claimed in claim 27, wherein the digital pen is configured to generate at least one encryption key using a random seed based on a physical parameter of a sensor of the digital pen.